30 Aralık 2021

bLOKCHAİN HACKATHON

İçindekiler

[1. PROJENİN AMACI 1](#_Toc91699625)

[2. KULLANILAN TEKNOLOJİLER 1](#_Toc91699626)

[2.1. ASP.NET MVC 1](#_Toc91699627)

[2.2. ENTITY FRAMEWORK 1](#_Toc91699628)

[2.3. PYTHON 1](#_Toc91699629)

[2.4. BOOTSTRAP 2](#_Toc91699630)

[2.5. SQL 2](#_Toc91699631)

[2.6. VISUAL STUDIO 2019 2](#_Toc91699632)

[2.7. VISUAL STUDIO CODE 3](#_Toc91699633)

[2.8. SQL SERVER 2014 MANAGEMENT STUDIO 3](#_Toc91699634)

[2.9. POSTMAN 3](#_Toc91699635)

[3. PROJE GEREKSİNİMLERİ 3](#_Toc91699636)

[3.1. Python 3](#_Toc91699637)

[GENEL İSTERLER 3](#_Toc91699638)

[dilKontrol SINIFI İSTERLERİ 4](#_Toc91699639)

[sifrelemeYontemleri SINIFI İSTERLERİ 4](#_Toc91699640)

[Help SINIFI İSTERLERİ 4](#_Toc91699641)

[3.2. Veritabanı Yönetim Sistemleri 4](#_Toc91699642)

[Veritabanı Tasarımı 4](#_Toc91699643)

[View, Stored procedure ve tanımlı fonksiyon kullanımı 4](#_Toc91699644)

[3.3. İleri Web Programlama 5](#_Toc91699645)

[4. EMEĞİ GEÇENLER 6](#_Toc91699649)

# PROJENİN AMACI

Bu proje içerisinde temel olarak kullanılan Transaction, Transaction’lardan oluşan Block, ve Block’ların oluşturduğu Blockchain, ikili anlaşmalar sırasında gerçeklenen her Transaction’ın şifrelenmesi ve doğrulaması Asymmetric Encryption algoritması kullanılarak projenin tamamlanması amaçlanmıştır.

# KULLANILAN TEKNOLOJİLER

# ASP.NET MVC

ASP veya ASP. NET, web ve masaüstü uygulamaları oluşturmak için kullanılan bir çerçevedir. ASP yazılımı formlar veya web uygulamaları halinde gelir ve bu programlar Microsoft'un geliştirici platformu olan Visual Studio’da geliştirilir. ASP yazılımı, kurumsal veya küçük ofis ortamlarında bir Windows masaüstü bilgisayarında veya web barındırma sunucusunda çalışır.

# ENTITY FRAMEWORK

Microsoft tarafından desteklenen .NETuygulamaları için açık kaynaklı bir ORM çerçevesidir. Yazılım geliştiricilerin, bu verilerin depolandığı temel veritabanı tablolarına ve sütunlarına odaklanmadan, alana özgü sınıfların nesnelerini kullanarak verilerle çalışmasını sağlar. Veri üzerinde çalışılırken daha yüksek bir soyutlama(isolation) sağlanabilir ve geleneksel uygulamalara göre daha az satır kodla veri odaklı uygulamalar oluşturulabilir. Entity Framework (Tanım): .NET geliştiricilerinin .NET nesneleri kullanarak bir veritabanıyla çalışmasını sağlayan, geliştiricilerin genellikle yazması gereken çoğu veri erişim koduna olan ihtiyacı ortadan kaldıran nesne-ilişkisel bir eşleyicidir (O/ RM).

# PYTHON

Python, nesne yönelimli, yorumlamalı, birimsel (modüler) ve etkileşimli yüksek seviyeli bir programlama dilidir.

Girintilere dayalı basit söz dizimi, dilin öğrenilmesini ve akılda kalmasını kolaylaştırır. Bu da ona söz diziminin ayrıntıları ile vakit yitirmeden programlama yapılmaya başlanabilen bir dil olma özelliği kazandırır.

Modüler yapısı, sınıf dizgesini (sistem) ve her türlü veri alanı girişini destekler. Hemen hemen her türlü platformda çalışabilir (Unix, Linux, Mac, Windows, Amiga, Symbian). Python ile sistem programlama, kullanıcı arabirimi programlama, ağ programlama, web programlama, uygulama ve veri tabanı yazılımı programlama gibi birçok alanda yazılım geliştirebilirsiniz. Büyük yazılımların hızlı bir şekilde prototiplerinin üretilmesi ve denenmesi gerektiği durumlarda da C ya da C++ gibi dillere tercih edilir.

**SHA-3**

SHA-3, en yeni NIST güvenli karma algoritma standardıdır. Daha büyük sayıya rağmen SHA-3, SHA-2'den daha iyi olarak kabul edilmez. Bunun yerine, önemli ölçüde farklı bir iç yapı kullanır, böylece SHA-2'ye karşı bir saldırı ortaya çıkarsa, SHA-3'e uygulanması pek olası değildir. SHA-3, SHA-2'den önemli ölçüde daha yavaştır, bu nedenle şu anda çoğu kullanıcı SHA'yı seçmelidir.

**BLAKE2**

BLAKE2, RFC 7693'te belirtilen bir şifreleme karma işlevidir. BLAKE2'nin tasarımı, onu, SHA karma ailesine göre bir avantaj olarak, uzunluk uzatma saldırılarına karşı bağışık hale getirir.

**SHA-1**

SHA-1, NIST tarafından standartlaştırılmış bir şifreleme karma işlevidir. 160 bitlik bir mesaj özeti üretir. SHA-1'in şifreleme analizi, pratik çarpışma saldırılarına karşı savunmasız olduğunu göstermiştir ve çarpışmalar kanıtlanmıştır.

**MD5**

MD5, kullanımdan kaldırılmış bir şifreleme karma işlevidir. 128 bitlik bir mesaj özeti üretir ve bilinen pratik çarpışma saldırılarına sahiptir.

**Asymmetric**

Python'da Şifreleme ve Şifre Çözme ile ilgili makalemi okursanız, şifrelemek ve şifresini çözmek için yalnızca bir anahtar kullandığımı görürsünüz.

Asimetrik şifreleme iki anahtar kullanır- bir özel anahtar ve bir genel anahtar. Herkese açık anahtarlar herkesin kullanması için verilir, siz onları herkese açık bilgi haline getirirsiniz. Herkes ortak anahtarınızla verileri şifreleyebilir ve ardından yalnızca özel anahtara sahip olanlar mesajın şifresini çözebilir. Bu aynı zamanda tersi şekilde de çalışır, ancak özel anahtarınızı gizli tutmak için bir kuraldır.

**Symmetric**

Simetrik şifreleme, hem göndericinin hem de alıcının aynı gizli anahtarı kullandığı materyalin içeriğini şifrelemenin veya gizlemenin bir yoludur. Simetrik şifrelemenin çoğu uygulama için yeterli olmadığını unutmayın, çünkü yalnızca gizlilik sağlar, ancak özgünlük sağlamaz. Bu, bir saldırganın mesajı göremediği, ancak bir saldırganın sahte mesajlar oluşturabileceği ve uygulamayı bunların şifresini çözmeye zorlayabileceği anlamına gelir. Birçok bağlamda, şifreli mesajlarda kimlik doğrulama eksikliği, gizlilik kaybına da neden olabilir.

**SHA2**

SHA-2 (Secure Hash Algorithm 2), Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (NSA) tarafından tasarlanan ve ilk kez 2001'de yayınlanan bir dizi kriptografik hash işlevidir. Bunlar, tek yönlü bir sıkıştırma işlevinden Merkle–Damgård yapısı kullanılarak oluşturulmuştur. Kendisi özel bir blok şifrelemeden Davies-Meyer yapısı kullanılarak inşa edilmiştir.

SHA-2, selefi SHA-1'den önemli değişiklikler içerir. SHA-2 ailesi, 224, 256, 384 veya 512 bit olan özetlere (karma değerleri) sahip altı karma işlevinden oluşur: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA -512/256. SHA-256 ve SHA-512, sırasıyla sekiz 32-bit ve 64-bit word ile hesaplanan yeni hash fonksiyonlarıdır. Farklı kaydırma miktarları ve katkı sabitleri kullanırlar, ancak yapıları, yalnızca tur sayısında farklılık gösteren, hemen hemen aynıdır. SHA-224 ve SHA-384, farklı başlangıç ​​değerleriyle hesaplanan, sırasıyla SHA-256 ve SHA-512'nin kesilmiş sürümleridir. SHA-512/224 ve SHA-512/256 da SHA-512'nin kısaltılmış sürümleridir, ancak ilk değerler, Federal Bilgi İşleme Standartları (FIPS) PUB 180-4'te açıklanan yöntem kullanılarak oluşturulur.

# BOOTSTRAP

Twitter Bootstrap (ya da kısaca Bootstrap) açık kaynak kodlu, web sayfaları veya uygulamaları geliştirmek için kullanılabilecek araçlar bütünü ve önyüz çatısı. Bootstrap, web sayfaları veya uygulamalarında kullanılabilecek, HTML ve CSS tabanlı tasarım şablonlarını içerir. Bu şablonlar form, navigasyon çubuğu, buton gibi arayüz bileşenleri oluşturmakta kullanılabilmektedir. Ocak 2021 itibarı ile Bootstrap, Github üzerinde 148 binin üzerinde "star" ile 71 binin üzerinde "fork" sayılarına ulaşarak, sitenin en popüler projelerinden biri olmuştur.

# SQL

SQL, verileri yönetmek ve tasarlamak için kullanılan bir dildir. SQL, kendisi bir programlama dili olmamasına rağmen birçok kişi tarafından programlama dili olarak bilinir. SQL herhangi bir veri tabanı ortamında kullanılan bir alt dildir. SQL ile yalnızca veri tabanı üzerinde işlem yapılabilir; veritabanlarında bulunan sistemlere bilgi ekleme, bilgi değiştirme, bilgi çıkarma ve bilgi sorgulama için kullanılmaktadır. Özellikle de ilişkisel veritabanı sistemleri üzerinde yoğun olarak kullanılmaktadır. SQL'e özgü cümleler kullanarak veri tabanına kayıt eklenebilir, olan kayıtlar değiştirilebilir, silinebilir ve bu kayıtlardan listeler oluşturulabilir.

# VISUAL STUDIO 2019

Microsoft Visual Studio, Microsoft tarafından geliştirilen bir tümleşik geliştirme ortamıdır (IDE). Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, .NET Compact Framework ve Microsoft Silverlight tarafından desteklenen tüm platformlar için yönetilen kod ile birlikte yerel kod ve Windows Forms uygulamaları, web siteleri, web uygulamaları ve web servisleri ile birlikte konsol ve grafiksel kullanıcı arayüzü uygulamaları geliştirmek için kullanılır.

Visual Studio IntelliSense'in yanı sıra "code refactoring" destekleyen bir kod editörü içerir. Entegre hata ayıklayıcı, hem kaynak-seviyesinde hem de makine-seviyesinde çalışır. Diğer yerleşik araçlar, GUI uygulamaları, web tasarımcısı, sınıf tasarımcısı ve veritabanı şema tasarımcısı yaratabilmek için bir form tasarımcısı içerir. Hemen hemen her işlevsellik düzeyinde dahil olmak üzere, kaynak kontrol sistemleri için destek (Subversion ve Visual SourceSafe gibi) sunan eklentileri kabul eder.

# VISUAL STUDIO CODE

Visual Studio Code Microsoft tarafından Windows, Linux ve MacOS için geliştirilen bir kaynak kodu düzenleyicisidir. Hata ayıklama, gömülü Git kontrolü, sözdizimi vurgulama, akıllı kod tamamlama, snippet'ler ve kod yeniden yapılandırma desteği içerir. Ayrıca özelleştirilebilir, böylece kullanıcılar editörün temasını, klavye kısayollarını ve tercihlerini değiştirebilir.Resmi indirme işlemi tescilli bir lisans altında olmasına rağmen, ücretsiz ve açık kaynaktır.

# SQL SERVER 2014 MANAGEMENT STUDIO

Sql server management ise Microsoft geliştirdiği bir database editörüdür. Bu editör yardımıyla T-SQL komutlarını kullanarak datalarımız üzerinde birçok farklı (data düzenleme, raporlama ve analiz gibi.) işlemler yapabiliriz. Bu programlar aracılığı ile MSSQL tipinde bir veritabanı oluşturur, veritabanını tasarlar, gerekli ayarları yaparsınız. Yani kısacası veritabanı tasarımı yaparsınız.

T-SQL, MS SQL Server veritabanı üzerinde işlemler (veri eklemek, değiştirmek, sorgulamak veya silmek) gerçekleştirmek için kullanılan sorgulama dilidir. Bir programlama dili olmasada programlama dillerine benzeyen bir alt dildir. Diğer veri tabanlarında da kullanılan dil aynıdır. Örneğin My Sql, Oracle gibi veri tabanları üzerinde de aynı dil yapısıyla sorgulama işlemleri yapabilirsiniz.

# POSTMAN

Postman, Chrome uzantısı olarak kullanabileceğimiz veya direct indirip bilgisayarımıza yükleyebileceğimiz bir uygulamadır. Rest Client olarak da tanımlanabilir.

API(Application Programming Interface) farklı uygulama yazılımlarının birbirleri ile etkileşim sağlamasına olanak sağlar. Client(Android) ve Backend(java) yazılımlarının Restfull Api ile iletişim kurması buna örnek verilebilir.

Postman sayesinde uzun uzun kodlar yazmak yerine API’lerimizi kolayca test edebiliriz. Birçok özelliği sayesinde kolay bir şekilde istek hazırlayıp gelen cevap değerlerini kullanabiliriz.

# PROJE GEREKSİNİMLERİ

## Python

### GENEL İSTERLER

Her sınıfın kendisine ait init fonksiyonu olmak zorundadır.

Sınıflar içerisinde yazılan fonksiyonlar parametre almalı, parametre geri döndürmelidir. (help sınıfı hariç)

En az 2 farklı yerde istisnalar (exception) kullanılmalıdır.

### dilKontrol SINIFI İSTERLERİ

İçerisinde 5 farklı fonksiyon bulundurması gerekmektedir.

Parametre olarak aldığı string ifadeleri varsa, cümlelere ve kelimelere ayıran iki fonksiyon bulunmak zorundadır. Parametre olarak cümle sayısı ve kelime sayılarını ayrı fonksiyonlarda döndürmelidir.

String ifade içerisinde kaç adet sesli harf olduğunu bulan fonksiyon bulunmak zorundadır. Parametre olarak toplam sesli harf sayısını döndürmelidir.

Kelimelerin büyük ünlü uyumuna uyup uymadığını kontrol eden bir fonksiyon bulunmak zorundadır. Parametre olarak büyük ünlü uyumuna uyan kelime sayısı ve uymayan kelime sayısını döndürmelidir.

### sifrelemeYontemleri SINIFI İSTERLERİ

En az 8 farklı fonksiyonu içermesi gerekmektedir.

Fonksiyonlardan en az 5 tanesi hash şifreleme yöntemi içermelidir.

Fonksiyonlardan en az 2 tanesi simetrik veya asimetrik şifreleme yöntemi içermelidir.

### Help SINIFI İSTERLERİ

Bu sınıf çalıştırıldığında otomatik olarak ekrana modülü ve modülün içerisindeki fonksiyonları anlatan bir yazı ekrana gelmelidir.

## Veritabanı Yönetim Sistemleri

### Veritabanı Tasarımı

Normalizasyon içeren uygun varlık ilişki modelinin belirlenmesi (10 puan)

En az 6 tablo kullanımı (10 puan)

Veri bütünlüğünü sağlamak adına uygun anahtar ve cascading stratejisi kullanımı (10 puan)

Veri bütünlüğü için en az 5 adet constraint (kısıt) kullanımı (10 puan)

(En az 1 check constraint, 1 default constraint ve 1 unique constraint kullanılmalıdır)

Veri bütünlüğü için en az 2 adet rule kullanımı (10 puan)

### View, Stored procedure ve tanımlı fonksiyon kullanımı

En az 2 stored procedure (10 puan)

En az 3 view kullanımı (10 puan)

En az 2 kullanıcı tanımlı fonksiyon kullanımı (10 puan)

En az 1 adet trigger kullanımı (10 puan)

Ön yüz tasarımı (10 puan)

## İleri Web Programlama

Front end için iyi bir tasarım (20 puan)

Veritabanı (Database) kullanımı (20 puan)

ASP.NET MVC ile backend yazımı (20 puan)

Autherization/Authentication kullanımı (Session veya Token) (20 puan)

Entity Framework Kullanımı veya Database Access Layer yazımı (20 puan)

# EMEĞİ GEÇENLER

Oytun TUR 192802012

Serdar SAVAŞ 192802014

Ömer Fikri GÜLCEMAL 192802009

Ulaş CANIMOĞLU 192802039

Ahmet CEYRAN 192802057

Dicle ACET 192803044